计算机工程与应用 2008 44 (15): 103-105 ISSN: 1002-8331 CN: 11-2127/TP

网络、通信、安全

基于NTRU的3G移动通信认证和密钥分配方案

赖 欣[1], 黄晓芳[2], 何大可[1]
1.西南交通大学 信息安全与国家网格计算实验室，成都 610031
2.北京邮电大学 信息安全中心，北京 100876

收稿日期 2007-8-30 修回日期 2007-10-16 网络版发布日期 2008-5-16 接受日期

摘要 指出3GPP提出的3G认证和密钥分配方案存在的安全漏洞。针对存在安全问题提出一个基于NTRU公钥密码体制的3G认证和密钥分配方案，该方案中将原认证和分配方案进行明文传输的身份信息与各安全参数用NTRU公钥加密算法进行加密保护，防止了恶意攻击者对身份信息以及安全参数的伪造与篡改，提高了认证和密钥分配方案的安全性和可靠性。同时该方案保持了原认证方案的结构模式，易于从原方案进行扩展实现。由于NTRU公钥密码方案在计算开销和带宽开销上的优势，使得该方案能在计算资源与存储资源都相对有限的移动通信网络环境下实现。

关键词 3G NTRU公钥密码体制 用户认证 密钥分配
分类号

3G authentication and key agreement scheme based on NTRU

LAI Xin[1],HUANQ Xiao-fang[2],HE Da-ke[1]

1.Information Security and National Computing Grid Laboratory（IS&NC）, Southwest Jiaotong University, Chengdu 610031, China
2.Information Security Center, Beijing University of Post and Telecommunications, Beijing 100876, China

Abstract
The security defects of 3GPP authentication and key agreement scheme are pointed out.To solve these defects a new 3G authentication and key agreement scheme based on NTRU public cryptography is proposed.In the new scheme user's identities and security parameters are encrypted by NTRU encryption algorithm to avoid adversary forge or tamper these information, which enhances the security and reliability of scheme.At same time the new scheme keeps the structure of previous scheme.So it's easily to achieve the new scheme by extending previous scheme.Owing to the computing and overhead advantage of NTRU, the new scheme can be realized in mobile communication environments limited in computing and memory resource.

Key words 3G NTRU public key cryptography user authentication key agreement

DOI:

通讯作者 赖 欣 lxswjtu@163.cm